PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

THE ACM DIGITAL LIBRARY

Feedback

intrusion alarms false positive
Terms used: intrusion alarms false positive

Fou

Sort results by: relevance

Save results to a Binder

Display results: expanded form

□ Open results in a new window

Refine these results with Ad
Try this search in The ACM (

Results 1 - 20 of 200 Result page: 1 2 3 4 5 6 7 8 9 10 next >>

1 Measuring intrusion detection capability: an information-theoretic approach
Guofei Gu, Prahlad Fogla, David Dagon, Wenke Lee, Boris Skorić
March 2006 ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security
Publisher: ACM
Full text available: pdf(381.84 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 20, Downloads (12 Months): 367, Citation Count: 1

A fundamental problem in intrusion detection is what metric(s) can be used to objectively evaluate an intrusion detection system (IDS) in terms of its ability to correctly classify events as normal or intrusive. Traditional metrics (e.g., true positive ...

Keywords: information-theoretic, intrusion detection, performance measurement

2 Alert aggregation in mobile ad hoc networks
Bo Sun, Kui Wu, Udo W. Pooch
September 2003 WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security
Publisher: ACM
Full text available: pdf(207.57 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 179, Citation Count: 2

In Intrusion Detection Systems (IDSs) for Mobile Ad hoc NETworks (MANETs), IDS agents using local detection engines alone may lead to undesirable performance due to the dynamic feature of MANETs. In this paper, we present a nonoverlapping Zone-based ...

Keywords: alert aggregation, intrusion detection, mobile ad hoc networks, routing security

3 Network anomaly detection based on TCM-KNN algorithm
Yang Li, Binxing Fang, Li Guo, You Chen
March 2007 ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security
Publisher: ACM
Full text available: pdf(160.77 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 22, Downloads (12 Months): 425, Citation Count: 0

Intrusion detection is a critical component of secure information systems. Network anomaly detection has been an active and difficult research topic in the field of Intrusion Detection for many years. However, it still has some problems unresolved. They ...

Keywords: TCM-KNN algorithm, anomaly detection, machine learning, network security

4 Hybrid BP/CNN neural network for intrusion detection

Yao Yu, Gao Fu-xiang, Yu Ge

November 2004 InfoSecu '04: Proceedings of the 3rd international conference on Information security

Publisher: ACM

Full text available: pdf(161.90 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 62, Citation Count: 0

In order to improve the intrusion detection rates and reduce false positives, a hybrid BP/CNN neural network is constructed, which has both the capability of real-time classification which BP has and the functionality of time-delay, collection and judgment ...

Keywords: ROC curve, chaotic neuron, hybrid neural network, intrusion detection, time-delay classification

5 Experiences in passively detecting session hijacking attacks in IEEE 802.11 networks

Rupinder Gill, Jason Smith, Andrew Clark

January 2006 ACSW Frontiers '06: Proceedings of the 2006 Australasian workshops on Grid computing and e-research - Volume 54, Volume 54

Publisher: Australian Computer Society, Inc.

Full text available: pdf(573.69 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 17, Downloads (12 Months): 218, Citation Count: 0

Current IEEE 802.11 wireless networks are vulnerable to session hijacking attacks as the existing standards fail to address the lack of authentication of management frames and network card addresses, and rely on loosely coupled state machines. Even the ...

Keywords: passive monitoring, received signal strength, round trip time, session hi-jacking, wireless intrusion detection

6 Challenging the anomaly detection paradigm: a provocative discussion

Carrie Gates, Carol Taylor

September 2006 NSPW '06: Proceedings of the 2006 workshop on New security paradigms

Publisher: ACM

Full text available: pdf(145.52 KB) Additional Information: full citation, abstract, references

Bibliometrics: Downloads (6 Weeks): 31, Downloads (12 Months): 173, Citation Count: 1

In 1987, Dorothy Denning published the seminal paper on anomaly detection as applied to intrusion detection on a single system. Her paper sparked a new paradigm in intrusion detection research with the notion that malicious behavior could be distinguished ...

Keywords: intrusion detection, security

7 A service-centric approach to access control and monitoring based on distributed

trust
Jimmy McGibney, Dmitri Botvich
October 2007 CASCON '07: Proceedings of the 2007 conference of the center for advanced studies on Collaborative research
Publisher: ACM
Full text available: pdf(262.54 KB) Additional Information: full citation, abstract, references

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 45, Citation Count: 0

A service-oriented approach to dynamic refinement of security enforcement is described in this paper. This is based on a closed loop feedback system where live distributed trust measures are used to adapt access control settings in a changing threat ...

8 Modeling the emergence of insider threat vulnerabilities
Ignacio J. Martinez-Moyano, Eliot H. Rich, Stephen H. Conrad, David F. Andersen
December 2006 WSC '06: Proceedings of the 38th conference on Winter simulation
Publisher: Winter Simulation Conference
Full text available: pdf(233.69 KB) Additional Information: full citation, abstract, references

Bibliometrics: Downloads (6 Weeks): 12, Downloads (12 Months): 156, Citation Count: 0

In this paper, we present insights generated by modeling the emergence of insider threat vulnerabilities in organizations. In our model, we integrate concepts from social judgment theory, signal detection theory, and the cognitive psychology of memory ...

9 Estimating the detector coverage in a negative selection algorithm
Zhou Ji, Dipankar Dasgupta
June 2005 GECCO '05: Proceedings of the 2005 conference on Genetic and evolutionary computation
Publisher: ACM
Full text available: pdf(322.77 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 67, Citation Count: 4

This paper proposes a statistical mechanism to analyze the detector coverage in a negative selection algorithm, namely a quantitative measurement of a detector set's capability to detect nonself data. This novel method has the advantage of statistical ...

Keywords: detector coverage, hypothesis testing, negative selection

10 Immune anomaly detection enhanced with evolutionary paradigms
Marek Ostaszewski, Franciszek Seredynski, Pascal Bouvry
July 2006 GECCO '06: Proceedings of the 8th annual conference on Genetic and evolutionary computation
Publisher: ACM
Full text available: pdf(474.64 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 94, Citation Count: 0

The paper presents an approach based on principles of immune systems to the anomaly detection problem. Flexibility and efficiency of the anomaly detection system are achieved by building a model of network behavior based on the self-nonself space paradigm. ...

Keywords: artificial immune systems, coevolution, network anomaly detection

11 [redacted]

Keywords: Intrusion detection, cluster analysis, data mining, false positives, root cause analysis

12 Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory
November 2000 ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue 4
Publisher: ACM
Full text available: pdf(156.16 KB) Additional Information: full citation, abstract, references, cited by, index terms, review

Bibliometrics: Downloads (6 Weeks): 40, Downloads (12 Months): 394, Citation Count: 23

In 1998 and again in 1999, the Lincoln Laboratory of MIT conducted a comparative evaluation of intrusion detection systems (IDSs) developed under DARPA funding. While this evaluation represents a significant and monumental undertaking, there are a number ...

Keywords: computer security, intrusion detection, receiver operating curves (ROC), software evaluation

13 The base-rate fallacy and the difficulty of intrusion detection
Stefan Axelsson
August 2000 ACM Transactions on Information and System Security (TISSEC), Volume 3 Issue 3
Publisher: ACM
Full text available: pdf(124.41 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 23, Downloads (12 Months): 296, Citation Count: 15

Many different demands can be made of intrusion detection systems. An important requirement is that an intrusion detection system be effective; that is, it should detect a substantial percentage of intrusions into the supervised system, ...

Keywords: base-rate fallacy, detection rate, false alarm rate, intrusion detection

14 Intrusion detection techniques for mobile wireless networks
Yongguang Zhang, Wenke Lee, Yi-An Huang
September 2003 Wireless Networks, Volume 9 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(164.73 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 44, Downloads (12 Months): 565, Citation Count: 10

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. We ...

Keywords: anomaly detection, cooperative detection, intrusion detection, intrusion response, mobile ad-hoc networks

15 Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage

Jude Shavlik, Mark Shavlik

August 2004 KDD '04: Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining

Publisher: ACM

Full text available: pdf(192.20 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 9, Downloads (12 Months): 99, Citation Count: 1

We present and empirically analyze a machine-learning approach for detecting intrusions on individual computers. Our Winnow-based algorithm continually monitors user and system behavior, recording such properties as the number of bytes transferred over ...

Keywords: Windows 2000, Winnow algorithm, anomaly detection, feature selection, intrusion detection, machine learning, user modeling

16 Simple, state-based approaches to program-based anomaly detection

C. C. Michael, Anup Ghosh

August 2002 ACM Transactions on Information and System Security (TISSEC), Volume 5 Issue 3

Publisher: ACM

Full text available: pdf(459.57 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 145, Citation Count: 3

This article describes variants of two state-based intrusion detection algorithms from Michael and Ghosh [2000] and Ghosh et al. [2000], and gives experimental results on their performance. The algorithms detect anomalies in execution audit data. One ...

Keywords: Anomaly detection, finite automata, information system security, intrusion detection, machine learning

17 Anomalous system call detection

Darren Mutz, Fredrik Valeur, Giovanni Vigna, Christopher Kruegel

February 2006 ACM Transactions on Information and System Security (TISSEC), Volume 9 Issue 1

Publisher: ACM

Full text available: pdf(645.58 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 31, Downloads (12 Months): 418, Citation Count: 0

Intrusion detection systems (IDSs) are used to detect traces of malicious activities targeted against the network and its resources. Anomaly-based IDSs build models of the expected behavior of applications by analyzing events that are generated during ...

Keywords: Bayesian network, Intrusion detection, anomaly detection, computer security

18 Statistical profiling and visualization for detection of malicious insider attacks on computer networks
Jeffrey B. Colombe, Gregory Stephens
October 2004 VizSEC/ DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security
Publisher: ACM
Full text available: pdf(1.22 MB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 158, Citation Count: 1

The massive volume of intrusion detection system (IDS) alarms generated on large networks, and the resulting need for labor-intensive security analysis of the text-based IDS alarm logs, has recently brought into question the cost-effectiveness of IDSs. ...

Keywords: anomaly detection, cognitive load, human-computer interaction, information visualization

19 Distributed and control theoretic approach to intrusion detection
Rahul Khanna, Huaping Liu
August 2007 IWCMC '07: Proceedings of the 2007 international conference on Wireless communications and mobile computing
Publisher: ACM
Full text available: pdf(277.63 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 214, Citation Count: 0

Ad hoc wireless networks are more vulnerable to malicious attacks than traditional wired networks due to the silent nature of these attacks and the inability of the conventional intrusion detection systems (IDS) to detect them. These attacks operate ...

Keywords: IDS, hidden markov models, intrusion detection, wireless ad-hoc networks

20 Combining a bayesian classifier with visualisation: understanding the IDS
Stefan Axelsson
October 2004 VizSEC/ DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security
Publisher: ACM
Full text available: pdf(332.05 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 103, Citation Count: 1

Despite several years of intensive study, intrusion detection systems still suffer from two key deficiencies: Low detection rates and a high rate of false alarms. To counteract these drawbacks an interactive detection system based on simple Bayesian ...

Keywords: intrusion detection, naive bayesian classification

Results 1 - 20 of 200 Result page: 1 2 3 4 5 6 7 8 9 10 next >>

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player